(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－217033

(43)公開日　平成５年(1993)８月27日

(51)Int.Cl.[5]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｋ	19/073				
Ｇ０６Ｆ	12/14	３２０　Ｃ	9293－5B		
	15/30	３４０	6798－5Ｌ		
		３５０	6798－5Ｌ		
			8623－5Ｌ	Ｇ０６Ｋ　19/00　Ｐ	

審査請求　未請求　請求項の数８（全　８　頁）　最終頁に続く

(21)出願番号　特願平4－260878

(22)出願日　平成４年(1992)９月３日

(31)優先権主張番号　９１１０８８６

(32)優先日　1991年９月３日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　591032013

ジェムプリュス　カード　アンテルナショナル　ソシエテ　アノニム

GEMPLUS CARD INTERNATIONAL SOCIETE ANONYME

フランス国　13420　ジェムノ　パルク　ダクティヴィテ　ドゥ　ラ　プレーヌ　ドゥ　ジュク　アヴニュ　ドュ　ピック　ドゥベルターニュ（番地なし）

(74)代理人　弁理士　越場　隆

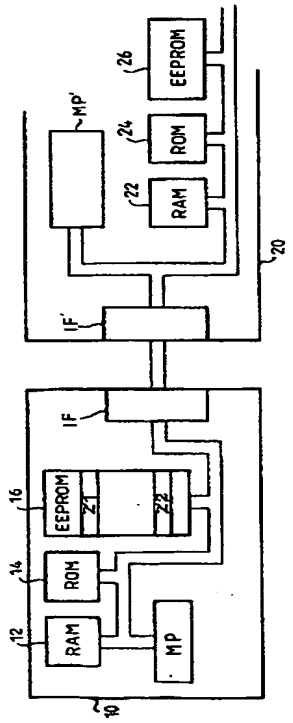
最終頁に続く

(54)【発明の名称】　データの認証方法

(57)【要約】

【目的】　例えば、チップカードの保有者にトランザクション装置がサービスを提供する前に、そのチップカードを認証することが必要な型の情報エレメントの認証方法が開示されている。

【構成】　認証は、情報の内容が本当にカード内に、カードのメモリの所定のアドレスに存在することを確認することからなる時、情報エレメントのブロックの長さをパラメータ化して、このブロックの暗号化アルゴリズムに、この長さに関するデータを内蔵することが提案される。すなわち、ブロックを含むファイルの論理アドレスとファイル内のブロックの位置がまた使用される。また、好ましくは、反復アルゴリズムが、Ｎ段階で実行される。認証すべきブロックは、一定の長さの複数のユニットに分割され、各段階で、そのユニットと前段階の結果の排他的ＯＲ関数を暗号化するデータとして使用する。



1

【特許請求の範囲】

【請求項１】　メモリ(16)の所定のファイルの所定のロケーションに含まれる情報エレメントブロックの形態の認証すべき情報エレメントと、暗号化すべきデータ（Ｄ）として、上記ファイルの論理アドレス、上記ブロックの位置及び長さ及びブロックの内容を介入させる暗号化プログラムとを使用する認証方法。

【請求項２】　上記暗号化プログラムは、認証すべき情報エレメントブロックと、そのサイズ及びその位置等の他の情報エレメントを含む情報エレメントの組のＮ個のユニットへの分割を設定し、次に、ユニット数Ｎを考慮して、暗号化プログラムを実施することを特徴とする請求項１に記載の方法。

【請求項３】　上記暗号化プログラムは、秘密のキーＫを有するアルゴリズムＣ（Ｄ、Ｋ）を使用し、そのアルゴリズムは、上記の認証すべき情報エレメントのブロック（Ｂ１）を所定のサイズのユニットに分割し、第ｎ番目のユニットは、d_n とし、段階ｎで、ユニットd_n 及び前段階ｎ－１でのアルゴリズムの実行の結果P_{n-1} を使用して情報エレメントについて上記暗号化アルゴリズムＣ（Ｄ、Ｋ）を反復的に実施することを含むことを特徴とする請求項１または２に記載の方法。

【請求項４】　各段階で、上記暗号化アルゴリズムをデータ片について実施し、上記暗号化アルゴリズムは、ユニットd_n と前段階ｎ－１でのアルゴリズムの実行の結果P_{n-1} との単純な論理結合、好ましくは、排他的ＯＲ結合であることを特徴とする請求項３に記載の方法。

【請求項５】　反復実行段階は、他のエレメントの中に、認証すべき情報エレメントのブロックの長さを備えるデータ片についてのアルゴリズムの実行であることを特徴とする請求項３または４に記載の方法。

【請求項６】　第１段階で、上記暗号化アルゴリズムは、秘密のキーＫによって暗号化すべきデータＤとして、上記情報エレメントブロックの位置及び長さの論理特性、上記ファイルの論理アドレス、及び、場合によってはランダム数を使用して、実施されることを特徴とする請求項５に記載の方法。

【請求項７】　上記認証されるべき情報エレメントは、メモリカード内にメモリに内蔵され、上記暗号化アルゴリズムは、上記カードのメモリ内に内蔵されたプログラムの制御下で該カードに内蔵されたマイクロプロセッサによって実行され、上記暗号化の結果は、上記カードの外部に転送されることを特徴とする請求項１～６のいずれか１項に記載の方法。

【請求項８】　上記暗号化アルゴリズムは、上記カードのメモリに内蔵された秘密のキーを使用し、該カードの外部には転送されない内容を有することを特徴とする請求項６に記載の方法。

【発明の詳細な説明】

【０００１】

2

【産業上の利用分野】本発明は、デジタル情報エレメントの処理の安全性に関するものである。さらに詳しく言えば、本発明は、ファイル内に内蔵された２進数情報エレメントを認証することができる新規な方法に関するものである。

【０００２】

【従来技術】「認証方法」という表現は、ここでは、ある場所で求められたデータの組が、実際に、予想されたデータの組であることが確認される信号処理動作であると理解されたい。求められたデータの組が予想されたデータの組である時、（他の動作の実行について）認証が出力される。そうでない場合、禁止が出力される。電子的な認証方法は、日々の生活での電子工学の使用が増加するにつれて、益々必要になっている。電子認証を使用して、正当な人が秘密の情報や専用の場所にアクセスすることができ、また、個人口座を使用して、信用価値を直接有するトランザクションを行うことができる。特に、サービスの提供の際の電子チップカード（ＩＣカード）の使用は、増加している。認証手続きは、チップカードが、そのようなサービスを提供する権限を実際に備えており、そのカード保有者が本当にこのカードの使用する権利があることを確認するのに必要である。本発明は、以下に、チップカードを例にして説明する。それによって、本発明をより容易に理解することができよう。しかし、本発明は、この例に限定されるものではない。

【０００３】以下に説明する認証方法の実例は、後で説明する本発明が利用できる種々の可能な状態を示す例として記載する。例えば、チップカードの場合、以下の認証の方法が広く使用されている。すなわち、カードは、内部の不揮発性メモリに、カードの保有者に固有で、その保有者しか知らない暗証コード（秘密コード）を内蔵している。このカードを、情報エレメントの入力のためのキーボードに接続された読取機に挿入する。カードの保有者は、キーボードを介して、暗証コードを入力する。この暗証コードは、カードに転送される。カード内で比較を行い、入力されたコードがメモリ内の秘密のコードと一致した時のみ後続の操作が可能になる。これは、認証の第１のレベル、すなわち、保有者の正当性の確認である。第２のレベルは、そのカードが、読取器が実施するトランザクションを実施する資格が本当にあるかどうかを確認することからなる。その時、このカードは、別の不揮発性メモリ領域に、暗号化アルゴリズムＣ（Ｄ、Ｋ）の秘密のキーＫ１を内蔵する。ここで、Ｃはデータ片Ｄ及びキーＫの関数である。保有者が知っていなければならない個人の暗証コードとは異なり、キーは、保有者には知られていない。カード読取機は、任意のデータ片Ｄ１をカードに送る。カードは、そのメモリ内に暗号化プログラムＣ（Ｄ、Ｋ）を内蔵している。そのプログラムは、秘密のキーＫ１によってデータＤ１を暗号化し、すなわち、関数Ｃ（Ｄ１、Ｋ１）を実行す

る。結果Ｒ１を読取機に送るが、一方、その読取機は、その間に、同じデータＤ１を同じ暗号化アルゴリズムＣ（Ｄ、Ｋ）とその読取機がそのメモリ内に有し、原則的には、Ｋ１に対応しなければならないキーＫ２で暗号化する。暗号化演算の結果Ｒ１及びＲ２を比較する。対応すれば、チップカード内に正しいキーＫ１が存在することを意味する。そうでない場合は、操作は許可されない。対応は、Ｒ１及びＲ２の一致検出であるが、また、一致検出ではない所定の関係の場合もある。

【０００４】例えば、別の認証方法では、結果Ｒ１を得るためにカード内で使用するアルゴリズムＣ（Ｄ、Ｋ）は、結果Ｒ２を得るために読取機内で使用されるアルゴリズムとは同じではない。例えば、カードのアルゴリズムは、結果Ｒ１を導く暗号化アルゴリズムＣ（Ｄ１、Ｋ１）である。読取機内に内蔵されたアルゴリズムは、Ｒ１からＤ１を再生する暗号解読アルゴリズムである。その暗号解読アルゴリズムは、Ｄ（Ｒ、Ｋ）と示される。公知の型のアルゴリズム（ＲＳＡ）を使用することができる。このアルゴリズムは、以下の特性を有する。すなわち、Ｋ１とは異なる単一のキーＫ２は、キーＫ１で暗号化された結果Ｒ１を解読することができる。これは、各キーＫ１ごとに、単一のキーＫ２は、Ｃ（Ｄ１、Ｋ１）＝Ｒ１であれば、Ｄ（Ｒ１、Ｋ２）＝Ｄ１であるようなものであることを意味する。そのとき、電子処理は以下の通りである。読取機は、データ片Ｄ１をカードに送る。カードは、このデータを、アルゴリズムＣ（Ｄ、Ｋ）で、その内部キーＫ１を使用して暗号化する。結果Ｒ１を読取機に送る。その読取機は、この結果Ｒ１に基づいて暗号解読アルゴリズムＤ（Ｒ１、Ｋ２）を実施する。その結果は、読取機によって最初に送られたデータＤ１と比較される。一致しなければ、カードに内蔵されているキーは正しいキーではないことを意味する。従って、この場合、確認されることは、２つの暗号化キーの一致ではなく、暗号化キーＫ１とそれに対応する唯一の暗号解読キーＫ２との間の対応があることである。この装置では、特に、暗号化キーを知っていても逆の暗号解読キーを計算するのに使用できなし、またその逆に、暗号解読キーを知っていても逆の暗号化キーを計算するのに使用できないので、２つのキーのうちの一方を保護しないですむアルゴリズムＲＳＡを使用する場合、高い安全性が得られる。これらの方法の安全性を高めるために、読取機によって送られるデータＤ１は、ランダム情報エレメントであり、従って、認証の際、一連の無駄な試みから結論を引き出すことはできない。

【０００５】上記の記述は、カード内にある秘密キーの存在によるカードの認証に関するものである。しかしながら、カードのメモリの内容の一部分は、カードとカード読取機との間の接続リンク上を明快な形で通過する内容を認証することなく、認証されなければならない場合が考えられる。この場合、例えば、秘密キーＫとして、カード内に内蔵されるキーを、データＤとして、カード読取機によって送られるデータ片ではなく（またはそのデータ片に加えて）カード内に含まれる情報片を使用することによって、秘密キーの暗号化アルゴリズムＣ（Ｄ、Ｋ）を実行することができる。この場合、もちろん、カード内に内蔵されており、アルゴリズムを実施するプログラムが、認証されるべき情報の位置を知る必要がある。この位置は、ファイル内の物理アドレスまたは論理アドレスによって示される。従って、キーとして、カード内に含まれている秘密キーを、データとして、特に予想された情報の内容である複数の情報エレメントと、それが位置していなければならない物理アドレスまたは論理アドレスと、場合によっては、カード読取機によって送られるデータ（例えば、ランダム情報エレメント）を使用して、暗号化アルゴリズムによって情報を認証することが提案される。実際、このようにして確認される情報エレメントは、一定の長さの情報エレメントであり、例えば、確認すべき情報は１つの４バイトワード、アドレスは１ワード及びランダム情報エレメントは１ワードである。

【０００６】

【発明が解決しようとする課題】本発明の目的は、１つの同じチップカード（チップカードの場合）を多数のアプリケーションに使用することができ、従って、１つの同じチップカードが極めて性質の異なる、認証すべき情報エレメントを含むことができるように、認証方法の可能性を大きくすることである。

【０００７】

【課題を解決するための手段】本発明によると、所定のファイルの所定のロケーションに内蔵された情報エレメントのブロックの形態の認証すべき情報エレメントと、情報エレメントブロック、ファイル内のデータブロックの位置と長さ、及び、情報エレメントブロックの実際の内容を、暗号化すべきデータとして使用する暗号化プログラムとを使用する認証方法が提案される。これによって、前もってサイズの決定された情報だけでなく、そのサイズとは無関係に、情報を認証することができる。従って、アプリケーションに応じてパラメータ化されるサイズを有する情報エレメントのブロックの認証を必要とする極めて様々なアプリケーションに１つの同じカードを使用することができるので、使用の柔軟性が大きくなる。一定の長さの情報エレメントを使用する暗号化プログラムの場合、暗号化すべき情報エレメントのブロックのサイズに関する情報は、その暗号化すべき情報を一定の長さのＮ個のユニット（小単位）に分割するのに使用される。暗号化操作は、各ユニットごとに実施される。従って、暗号化プログラムは、ブロックのサイズを考慮して、ブロックサイズとは無関係に暗号化を実施することができる。

【０００８】本発明の好ましい実施例では、暗号化プロ

5

グラムは、秘密キーＫを有するアルゴリズムＣ（Ｄ、Ｋ）を使用する。そのアルゴリズムは、反復して、以下のように、実施される。認証すべき情報エレメントのブロックを、所定のサイズのユニットに分割し、第ｎ番目のユニットはd_nとする。段階ｎで、ユニットd_n及び前の段階ｎ－１でのアルゴリズムの実行の結果P_{n-1}を介入させる情報エレメントについて、暗号化アルゴリズムＣ（Ｄ、Ｋ）を反復して実施する。好ましくは、各段階で、データ片について、暗号化アルゴリズムを実施する。その暗号化アルゴリズムは、ユニットD_nと前段階のアルゴリズムの実行の結果P_{n-1}との単純な論理結合、好ましくは、排他的ＯＲ結合である。アルゴリズムの反復実行の段階は、好ましくは、他のエレメントの中に、ブロックを含むファイルの論理アドレスと情報エレメントのブロックの位置及び長さとを含む情報エレメントのユニットに対するアルゴリズムの実行である。実際、アルゴリズムの反復実行の第１段階は、上記の情報エレメントについて、及び、場合によっては、アプリケーションから来る情報エレメント（一般的に、チップカードの場合はカード読取機から来る情報エレメント及び好ましくはランダム情報エレメント）について実施される。いずれの場合も、ファイルの論理アドレス及びブロックの位置と長さは、命令でカードに転送されるのであり、カードに書き込まれてはいないことが注目される。本発明のその他の特徴及び利点は、添付図面を参照して行う以下の詳細な説明から明らかになろう。

【０００９】

【実施例】本発明を実施例を参照して説明される。しかし、本明細書の冒頭に示したように、様々な状況が可能であるので、この実施例に限定されるものではない。図１には、主に、マイクロプロセッサＭＰと、このマイクロプロセッサに接続されたメモリと、カードと外部との間の通信に必要なインターフェースカードＩＦとを備えるメモリカード10が図示されている。マイクロプロセッサに接続されるメモリとしては、通常、作業用のランダムアクセスメモリ（ＲＡＭ）12と、プログラム用の読出専用メモリ（ＲＯＭ）14と、電気的にプログラム可能で且つ場合によっては電気的に消去可能な、不揮発性メモリ（ＥＰＲＯＭまたはＥＥＰＲＯＭ）16とを備える。メモリ16は、好ましくは、複数の領域に分割されており、そのいくつかは、外部から読み出すことができ、一方、他の領域は、外部から読み出すことができない（しかし、マイクロプロセッサだけが、それ自体の必要に応じて読み出すことができる）。更に、メモリ16は、プログラム可能な領域と、プログラム不可能な領域とに分割されてもよい。領域がプログラム不可能な場合、それは、所定の時に記録が既に実施されており、その後、書込みアクセスは物理的または論理的手段によって恒久的に阻止されることを意味する。カードは、トランザクション装置20と通信するように構成されている。その目的は、

6

カードの保有者がそのカードを装置に導入した時、カードの保有者にサービスを提供することである。本発明は、装置によるカードの認証に関する事項に限定されているので、サービスの提供に関して、装置の動作は説明しない。サービスは、どんなサービスであっても、カードの認証の成功した後でしか提供されない。トランザクション装置20は、もちろん、カード10の対応するインターフェースカードと通信することのできるインターフェースカードＩＦ’を備える。また、そのトランザクション装置は、好ましくは、カードの信号処理手段に類似の信号処理手段、すなわち、マイクロプロセッサＭＰ’と、作業用のランダムアクセスメモリ22と、プログラム用の読出専用メモリ24と、場合によって、不揮発性メモリ26とを備える。しかしながら、これらの手段は、所定のプロトコルによって（インターフェースＩＦ’を介して）カードと通信して、カードと情報を交換することのできるマイクロコンピュータまたはそれと等価な手段によって置き換えることができる。

【００１０】本実施例では、カードの認証は、カードの不揮発性メモリ16の所定のロケーションの領域Ｚ１の内容の確認を要求するものとする。トランザクション装置は、情報エレメントＢ１の所定のブロックがこのロケーションに存在することを確認する。もちろん、この確認は、情報エレメントを明快な形でカードと読取機との間を通過させないで、実施すべきである。メモリ領域Ｚ１は、カードの外部から、読出及び書込のどちらの場合もアクセス不可能にされている。しかしながら、読出専用メモリ（ＲＯＭ）14またはＥＥＰＲＯＭ16内に含まれているプログラム内に固定された所定の動作では、アクセスすることができる。トランザクション装置20は、ランダム情報エレメントＤ１を作製し、その情報エレメントをカードに送る。また、ファイルの論理アドレス、及び、本発明により、認証すべき情報エレメントのブロックＢ１のサイズと位置（このサイズは、例えば、バイト数またはワード数で算出される）を送る。そのプログラム用の読出専用メモリ内に含まれる暗号化アルゴリズムＣ（Ｄ、Ｋ）を使用することによって、カードは、情報エレメントのブロックの暗号化を実施し、そのブロックをトランザクション装置に転送する。トランザクション装置は、（実施例では）同じ情報エレメントについて同じ暗号化を実施する。暗号化のため、カードは、秘密のキーＫを使用する。このキーは、読出及び書込のどちらにもアクセス不可能なメモリ領域Ｚ２内にある。マイクロプロセッサだけがこの領域にアクセスすることができ、それは、暗号化アルゴリズムＣ（Ｄ、Ｋ）の実行中だけである。メモリ領域Ｚ２は、不揮発性メモリ16の一部分（原則的に）を形成する。本発明によると、秘密のキーによる暗号化が実施されるデータＤは、まず第１に、認証されるべき情報エレメントブロックを備え、第２に、このブロックのサイズ及び位置及びこのブロック

7

を含むファイルの論理アドレスを示すデータ片を備える。情報エレメントブロックが変えることのできるサイズを有する時、本発明の最も有望な特徴の一つはそこにあるので、サイズが可変であるという事実によって妨害されない暗号化アルゴリズムを使用することが望ましい。この理由のため、本発明では、カードに対してシステムが提供したブロックＢ１のサイズを使用して、暗号化プログラムでは、このサイズを考慮する。

【００１１】アルゴリズムＤＥＳ等の標準的な暗号化プログラムは、一定のサイズの情報エレメントについて作用し、一定のサイズの結果を出力する。この種のアルゴリズムによる暗号化を可能にするために、好ましくは、認証すべき情報エレメントのブロックを一定のサイズの複数のユニットに分割し、全てのユニットを処理するのに十分な数である複数の段階で暗号化演算を実施することが提案される。本発明の特徴によると、各段階で、認証すべきブロックの各ユニットごとではなく、所定のユニットと前段階で実施した演算の結果との単純な論理結合で、暗号化演算を実施することがが提案される。論理結合は、好ましくは、排他的ＯＲ結合である。すなわち、カードは、認証すべき情報エレメントブロックを一定のサイズのＮ個のユニットに分割する。その内容は、第ｎ番目のユニットでは、d_n である。段階ｎで実施した暗号化アルゴリズムＣ（Ｄ、Ｋ）は、結果P_n を提供する。この場合、各段階で、下記の計算が実施される。

P_n ＝Ｃ（d_n XOR P_{n-1} 、Ｋ）

（但し、（d_n XOR P_{n-1} ）は、 d_n とP_{n-1} との排他的ＯＲ結合を示すものとする。）もちろん、第１段階では、ｎは１に等しく、前段階の結果P_{n-1} は存在しない。計算は、情報エレメントの第１のユニットd_1 について直接実施できる。その時、式は、下記の通りである。

P_1 ＝Ｃ（d_1 、Ｋ）

好ましくは、情報エレメントの第１のユニットは、ファイルの位置とサイズ、及び、ファイルの論理アドレス、及び、必要ならば、アプリケーションによって与えられたランダム数Ｄ１の識別を可能にする論理特性を含む。従って、これらの論理特性は、以下の一連の表示を備える。

Ｒｄ：　ブロックＢ１を含むデータのファイルが存在するディレクトリの型、例えば、１バイト

Ｎｆ：　このディレクトリ中のファイルの数、例えば、１バイト

ｐ０：　ファイルの開始の関する情報エレメントブロックＢ１の位置、例えば、１バイト

Ｌ１：　ブロックＢ１の長さ、例えば、１バイト

Ｄ１：　トランザクション装置によって与えられるランダム情報エレメント、例えば、４バイト

それ故、その最初のユニットは、例えば、８バイトを備える。

8

d_1 ＝Ｔｄ、Ｎｆ、ｐ０、Ｌ１、Ｄ１

他のユニットは、情報エレメントブロックＢ１の８バイトに続く部分である。排他的ＯＲ演算は、ユニット分け演算のユニットの長さを維持する。

【００１２】通常の暗号化アルゴリズム（ＤＥＳ、ＲＳＡ）は暗号化情報エレメントと同じサイズの結果を提供するので、反復段階のシーケンスは、毎回、同じ長さの情報エレメントに関する。ここに、より詳細に記載する例では、Ｃ（Ｄ、Ｋ）に使用されるアルゴリズムは、アメリカ合衆国規格局(National Bureau of Standards of the United States of America)によって公開されたアルゴリズムＤＥＳである。その詳細な説明は、この組織または「フェデラル　レジスター(Federal Register)」第40巻、第52号（1975年３月17日）及び第40巻、第149号（1975年８月１日）から得ることができる。要するに、カードの読出専用メモリ14に内蔵されている暗号化プログラムによって、マイクロプロセッサは、最初に、暗号化すべき情報エレメントブロック（ブロックＢ１＋アドレス、位置及びサイズについての情報エレメント＋ランダム情報エレメントＤ１）をＮ個のユニットに分割し、次に、前もって測定したユニットの数を考慮して、実際の反復暗号化処理を実施する。上記の一連の反復段階の最後の結果P_N は、また、トランザクション装置に転送される。トランザクション装置は、同じ計算を実施し、カードの認証のためにその結果を比較する。図３のフローチャートは、カードの読出専用メモリ14内に内蔵され、トランザクション装置20が必要な情報エレメントを転送するとすぐにマイクロプロセッサによって実施される認証プログラムの主な段階の概要図である。可変のブロック長を使用して、メモリカード等の素子を認証することのできる独創的な解決法について、これまで記載してきた。情報ブロックが予想された論理特性（ファイルの位置、サイズ及び論理アドレスに関して）及び予想された内容を持たない時、この解決方法によって、認証が阻止される。

【図面の簡単な説明】

【図１】　認証すべき情報エレメントを含むメモリカードを使用するシステムの１実施例を図示したものである。

【図２】　認証のために使用される情報エレメントのブロックの分割の概略的な形態の図面である。

【図３】　認証を可能にする暗号化プログラムのフローチャートである。

【符号の説明】

10　メモリカード

12、22　ＲＡＭ

14、24　ＲＯＭ

16、26　ＥＥＰＲＯＭ

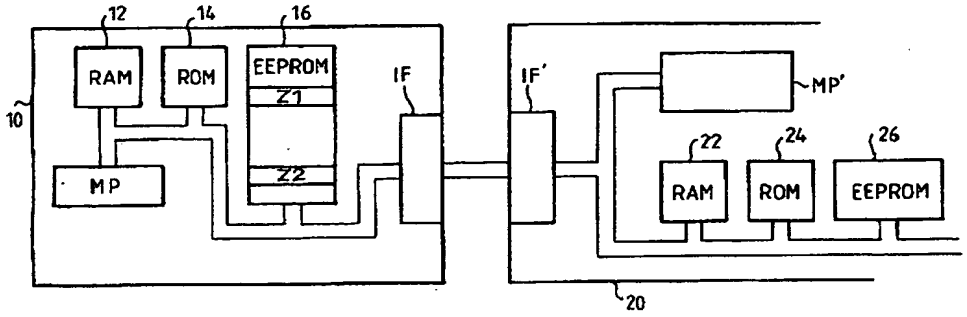
20　トランザクション装置

50　ＭＰ、ＭＰ’　マイクロプロセッサ

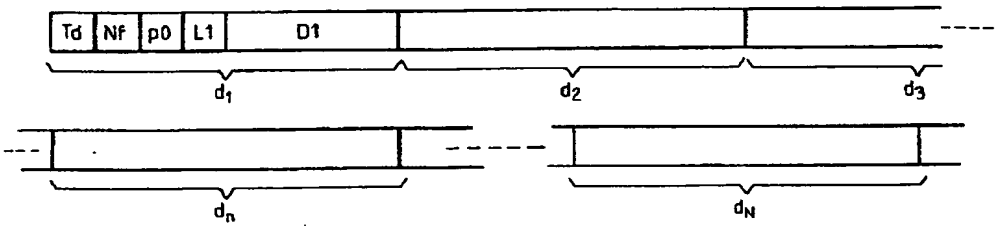
9　　10

ＩＦ、ＩＦ’　インターフェースカード

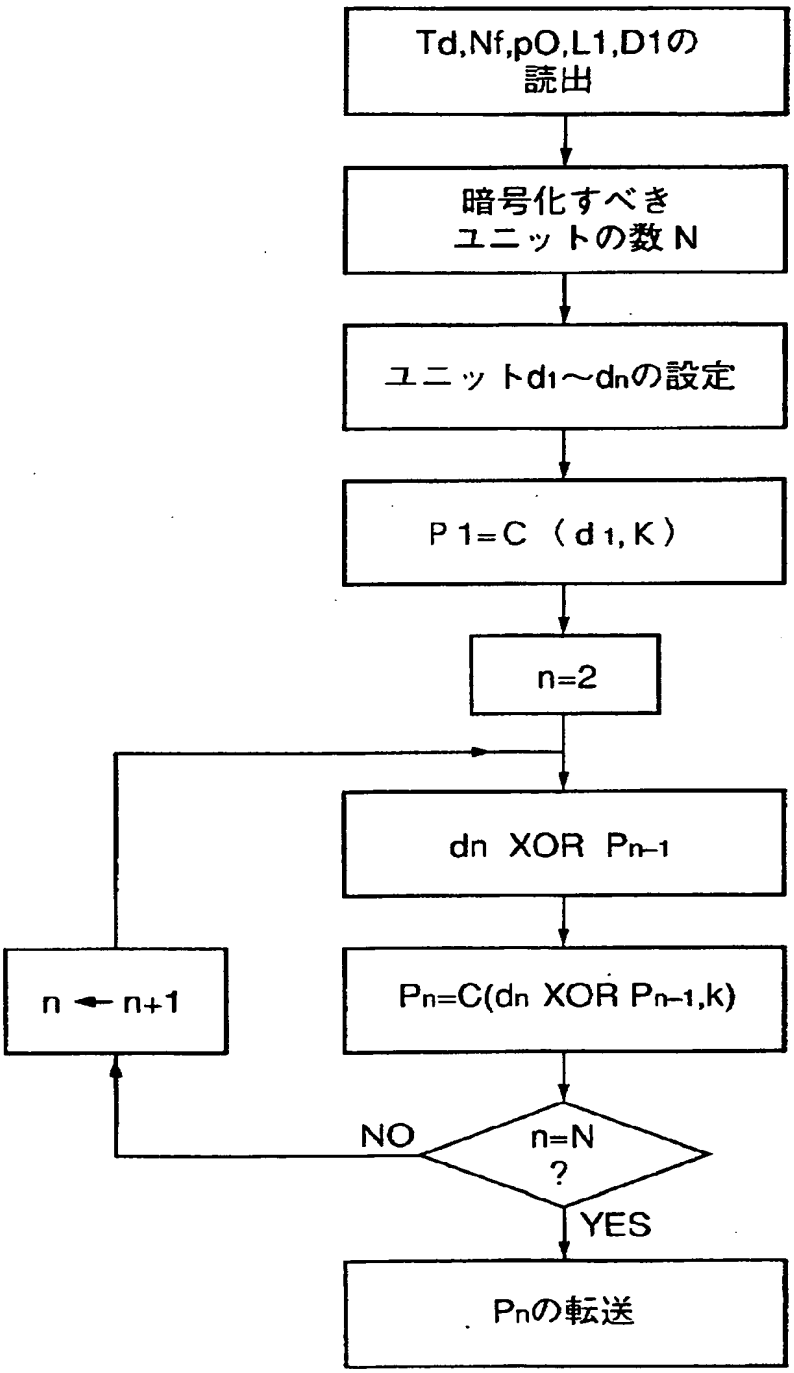
【図１】



【図２】



【図３】



フロントページの続き

(51) Int.Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/32				

(72)発明者　ジル　ヴィリセル
フランス国　13360　ロクヴェール　シュマン　ドゥ　バッサン　ヴィラ　マドレーヌ　（番地なし）